



Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.



Know the warning signs

In tax-related identity theft, the criminal generally will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season.

You may be unaware that this has happened until you file your return later in the filing season and discover that two returns have been filed using the same SSN.

Be alert to possible identity theft if you receive an IRS notice or letter that states:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages from an employer unknown to you.

Steps for victims of identity theft

1. File a report with the local police.
2. File a complaint with the Federal Trade Commission at www.identitytheft.gov or the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.
3. Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
 - www.Equifax.com 1-800-525-6285
 - www.Experian.com 1-888-397-3742
 - www.TransUnion.com 1-800-680-7289

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, take these additional steps:

4. Respond immediately to any IRS notice; call the number provided

5. Complete IRS [Form 14039, Identity Theft Affidavit](https://www.irs.gov/identitytheft). Use a fillable form at IRS.gov, print, then mail or fax according to instructions.

6. Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact the Identity Protection Specialized Unit at 1-800-908-4490. We have teams available to assist.

More information: www.irs.gov/identitytheft or FTC's www.identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft."

How you can reduce your risk

- Don't routinely carry your Social Security card or any document with your SSN on it.
- Don't give a business your SSN just because they ask – only when absolutely necessary.
- Protect your personal financial information at home and on your computer .
- Check your credit report annually.
- Check your Social Security Administration earnings statement annually.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Don't give personal information over the phone, through the mail or the Internet unless you have either initiated the contact or are sure you know who is asking.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

- No provea información personal a través del teléfono, por correo o por Internet a menos que sea usted quien inicia la comunicación y esté seguro de saber con quién está tratando.

Recuerde, el IRS no inicia comunicación con los contribuyentes vía correo electrónico para solicitar información personal ni información financiera. Esto incluye todo medio de comunicación electrónica, tal como los mensajes de texto y los canales de medios sociales.

¿Qué debe hacer si ha sido víctima de robo de identidad?

- Informe los incidentes de robo de identidad a la *FTC*, en www.consumer.gov/idtheft, o a la línea telefónica sobre el Robo de Identidad de la *FTC*, al 1-877-438-4338, o al 1-866-653-4261, si es usuario de equipo *TTY*.
- Presente un informe con la policía local.
- Comuníquese con el IRS y presente el Formulario 14039(SP), Declaración Jurada sobre el Robo de Identidad (o provea una copia del informe policial).
- Comuníquese con el departamento de fraude de las tres agencias nacionales de informe de crédito:
 - Equifax* – www.equifax.com 1-800-525-6285
 - Experian* – www.experian.com 1-888-397-3742
 - TransUnion* – www.transunion.com 1-800-680-7289
- Cierre toda cuenta que haya sido infiltrada o iniciada de manera fraudulenta.

¿Cómo puede saber si sus registros tributarios han sido afectados?

Normalmente, un ladrón de identidad utiliza la identidad legítima de un contribuyente para presentar fraudulentamente una declaración y reclamar un reembolso. Generalmente, el ladrón de identidad utiliza un número de Seguro Social robado para presentar una declaración con firma falsificada y así tratar de recibir un reembolso fraudulento a principios de la temporada de impuestos.

Quizás no sepa usted que esto está pasando hasta que presente su declaración más tarde en la temporada de impuestos y descubra que dos declaraciones han sido presentadas utilizando el mismo número de Seguro Social. Está pendiente de un posible robo de identidad si recibe una notificación o carta del *IRS* que le indique que:

- Más de una declaración de impuestos ha sido declarada a nombre suyo
- Usted tiene un saldo a pagar, un reembolso que ha sido aplicado a una deuda o alguna acción de cobro en contra de usted en un año en que no presentó una declaración de impuestos, o
- Los registros del *IRS* indican que usted recibió salarios de un empleador, el cual le es desconocido.

¿Cómo puede proteger sus registros tributarios?

Si en estos momentos sus registros tributarios no se ven afectados por el robo de identidad, pero usted cree que puede estar en riesgo debido a una cartera o billetera perdida o robada, por actividades cuestionables en una tarjeta de crédito o un informe de crédito, etc., comuníquese con la Línea Directa sobre la Unidad Especializada en Protección de Identidad, al 1-800-908-4490. Se le pedirá una copia del informe policial o usted tendrá que presentar el Formulario 14039(SP), Declaración Jurada sobre el Robo de Identidad, debidamente completado de acuerdo con las instrucciones en el dorso del mismo.

¿Qué debe hacer si sus registros se ven afectados por el robo de identidad?

Si usted recibe una notificación de parte del *IRS*, conteste inmediatamente. Si cree que alguien pudo haber utilizado su número de seguro social fraudulentamente, por favor, infórmelo al *IRS* inmediatamente, comunicándose al número y al nombre indicados en la carta o notificación.

Usted tendrá que completar el Formulario 14039(SP), Declaración Jurada sobre el Robo de Identidad. Escriba en forma legible y siga las instrucciones al dorso del formulario que corresponden a las circunstancias específicas de su caso.

Para las víctimas de robo de identidad que se han comunicado previamente con el *IRS* y no han logrado una solución, favor de comunicarse con la Unidad Especializada en Protección de Identidad del *IRS*, al número libre de cargos 1-800-908-4490.

¿Qué debe hacer si recibe un correo electrónico el cual dice provenir del IRS?

- Recuerde, el *IRS* no inicia comunicación con los contribuyentes vía correo electrónico. para solicitar información personal ni información financiera. Esto incluye todo medio de comunicación electrónica, tal como los mensajes de texto y los canales de medios sociales.
- Confirme que la correspondencia que recibió es de parte del *IRS*, llamando al 1-800-829-1040.
- Por favor, reenvíe dicho mensaje falso, supuestamente de parte del *IRS*, a phishing@irs.gov. Visite IRS.gov/espanol, palabra clave “*phishing*”, para obtener información detallada sobre cómo reenviar el correo electrónico.
- No abra los archivos adjuntos ni pulse sobre los enlaces dentro del correo electrónico falso.

Para información adicional, visite:

- IRS.gov/espanol (palabra clave: robo de identidad)
- IRS.gov/espanol (palabra clave: *phishing*)



Identity Theft Prevention and Victim Assistance

Prevención del Robo de Identidad y Ayuda para Víctimas

Information from the Internal Revenue Service

Información del Servicio de Impuestos Internos



English

The Federal Trade Commission, the lead agency on identity theft, reported that government documents/benefits fraud is the most common form of reported identity theft. At the IRS we take this issue very seriously.

What is identity theft?

Identity theft occurs when someone uses your personal information such as your name, Social Security number or other identifying information, without your permission, to commit fraud or other crimes.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years (as well as their hard earned money) repairing the mess thieves have made of their good name and credit record. Meanwhile, as a result of this financial fallout; victims may lose job opportunities, be refused loans, education, housing or transportation, and may even be arrested for crimes they didn't commit.

How can you minimize becoming a victim?

- Don't carry your Social Security card or any document(s) with your SSN on it.
- Don't give a business your SSN just because they ask - only when absolutely necessary. Question why it is needed and how it will be used.
- Protect your financial information.
- Check your credit report at least every 12 months.
- Secure personal information in your home.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches, and change passwords for Internet accounts.
- Don't give personal information over the phone, through the mail or on the Internet unless you have either initiated the contact or are sure you know who is asking.

Remember, the IRS does not initiate contact with taxpayers by email to request personal or financial information – this includes any type of electronic communication, such as text messages and social media channels.

What if you are a victim of identity theft?

- Report incidents of identity theft to the FTC at www.consumer.gov/idtheft, or the FTC Identity Theft hotline at 1-877-438-4338 or TTY 1-866-653-4261.
- File a report with the local police.
- Contact the IRS and file Form 14039, Identity Theft Affidavit (or provide a copy of the police report).
- Contact the fraud departments of the three major credit bureaus:

Equifax – www.equifax.com 1-800-525-6285

Experian – www.experian.com 1-888-397-3742

TransUnion – www.transunion.com 1-800-680-7289

- Close any accounts that have been tampered with or opened fraudulently.

How do you know if your tax records have been affected?

Usually, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity thief will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season.

You may be unaware that this has happened until you file your return later in the filing season and discover that two returns have been filed using the same SSN.

Be alert to possible identity theft if you receive an IRS notice or letter that states:

- More than one tax return for you was filed,
- You have a balance due, refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages from an employer unknown to you.

How can you protect your tax records?

If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity or credit report, etc., contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. You will be asked to provide a copy of a police report or you will need to submit a completed Form 14039, Identity Theft Affidavit, following the instructions on the back of the form.

What to do if your tax records were affected by identity theft?

If you receive a notice from the IRS, respond immediately. If you believe someone may have used your SSN fraudulently, please notify the IRS by responding to the name and number printed on the notice or letter. You will need to fill out the Form 14039, Identity Theft Affidavit. Please write legibly and follow the directions on the back of the form that relate to your specific circumstances.

For victims of identity theft who have previously been in contact with the IRS and have not achieved a resolution, please contact the IRS Identity Protection Specialized Unit, toll-free, at 1-800-908-4490.

What if you receive an e-mail claiming to be from the IRS?

- Remember, the IRS does not initiate contact with taxpayers by email to request personal or financial information – this includes any type of electronic communication, such as text messages and social media channels.

- Confirm the contact you have received is from the IRS by calling 1-800-829-1040.
- Please forward the bogus e-mail claiming to be from the IRS to phishing@irs.gov. Go to IRS.gov (keyword "phishing") to get instructions on how to forward the e-mail message.
- Do not open attachments or click on the links found within the bogus e-mail.

For additional information, visit:

- IRS.gov (keyword identity theft)
- IRS.gov (keyword phishing)

Spanish

La Comisión Federal de Comercio (*Federal Trade Commission*, o *FTC*, por sus siglas en inglés), la agencia principal encargada de combatir el robo de identidad, ha afirmado que el fraude relacionado con documentos y beneficios emitidos por el gobierno es la forma más común del robo de identidad denunciada a las autoridades. En el *IRS*, nosotros tomamos este asunto muy en serio.

¿Qué es el robo de identidad?

El robo de identidad ocurre cuando alguien utiliza su información personal, tal como su nombre, número de Seguro Social u otra información identificativa sin su permiso, para cometer fraude u otros crímenes.

El robo de identidad es un crimen serio. Las personas cuyas identidades han sido robadas pueden pasar meses o años, además de gastar grandes cantidades de dinero, intentando corregir los problemas que los ladrones crearon, dañando su buen nombre y registro de crédito. Mientras tanto, las víctimas se encuentran en apuros financieros y pueden perder oportunidades de trabajo, negárseles préstamos, educación, vivienda o automóviles, o aun ser arrestados por crímenes que no cometieron.

¿Cómo puede disminuir la posibilidad de ser una víctima?

- No lleve consigo su tarjeta de Seguro Social ni cualquier documento que muestre su número de Seguro Social.
- No provea su número de Seguro Social a un negocio simple mente porque se lo solicitan. Provea su número de Seguro Social sólo cuando sea absolutamente necesario. Pregúnteles por qué lo necesitan y cómo lo van a utilizar.
- Proteja su información financiera.
- Revise su informe de crédito cada 12 meses.
- Guarde su información personal en su hogar.
- Proteja su computadora personal utilizando cortafuegos (*firewalls*), software *anti-spam* y antivirus, actualice su sistema de seguridad y cambie sus contraseñas para las cuentas de Internet.